REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)
05-08-2008

2. REPORT TYPE
Final Report

3. DATES COVERED (From - To)
15-Jul-2005 - 14-Jul-2008

4. TITLE AND SUBTITLE WebBee: A Platform for Secure Coordination and Communication in ~~A~~ Crisis ~~Using Hand-held Devices~~ Scenarios

5a. CONTRACT NUMBER
W911NF-05-1-0415

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHORS
Sugih Jamin, Jignesh Patel, Morley Mao, Sarit Mukherjee, Liming Wang

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Michigan - Ann Arbor
Office of Sponsored Programs
Room 1058 Wolverine Tower
Ann Arbor, MI 48109 -1274

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
48770-CI-HRP.1

12. DISTRIBUTION AVAILIBILITY STATEMENT Approved for Public Release; Federal Purpose Rights
~~Distribution authorized to U.S. Government Agencies Only, Contains Proprietary information~~

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

Recently, disaster scenarios and terrorist attacks have made apparent some fundamental shortcomings in first responders' conventional coordination infrastructures. For example, unsatisfactory device connectivity, and security vulnerabilities made manifest by devices' inherently mobile nature, have the potential to seriously compromise first responders' effectiveness. To address these shortcomings, we designed and built Webbee, our secure coordination and communication infrastructure. In this article, we will take a high-level look at Webbee's architecture, and examine some interesting, non-trivial sample applications we have deployed on top of it.

15. SUBJECT TERMS
wireless security, COTS cellular networks, scalable spatial database, instant mobile network, disaster relief, GPS, challenge response, quorum

16. SECURITY CLASSIFICATION OF:

a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
U	U	U	SAR		Sugih Jamin
					19b. TELEPHONE NUMBER 734-763-1583

ABSTRACT

Recently, disaster scenarios and terrorist attacks have made apparent some fundamental shortcomings in first responders' conventional coordination infrastructures. For example, unsatisfactory device connectivity, and security vulnerabilities made manifest by devices' inherently mobile nature, have the potential to seriously compromise first responders' effectiveness. To address these shortcomings, we designed and built Webbee, our secure coordination and communication infrastructure. In this article, we will take a high-level look at Webbee's architecture, and examine some interesting, non-trivial sample applications we have deployed on top of it.

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

WebBee: A Platform for Secure Coordination and Communication in Crisis Scenarios, CrossTalk, The Journal of Defense Software Engineering, October 2008.

Number of Papers published in peer-reviewed journals: 1.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

Number of Papers published in non peer-reviewed journals: 0.00

(c) Presentations

DHS Semi-annual PI meetings.

Number of Presentations: 1.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

(d) Manuscripts

Number of Manuscripts: 0.00

Number of Inventions:

Graduate Students

NAME	PERCENT_SUPPORTED
Hyunseok Chang (9/30/05 - 3/9/06)	0.25
Yun Chen (7/31/05 - 12/31/07)	0.50
Wenjie Wang (9/1/05 - 4/30/06)	0.25
Zhiheng Wang (8/31/05)	0.25
Matthew England (8/31/05 - 8/31/06)	0.38
Axel Garcia Peña (6/1/06 - 8/26/06)	0.50
Todd Hopfinger (7/28/07-6/28/08)	0.50
Jeffrey Powers (1/31/06 - 12/13/07)	0.42
Patrick Turley (1/28/07 - 5/31/08)	0.50
John Umbaugh (9/30/07 - 6/30/08)	0.25
Krian Upatkoon (9/1/05 - 12/21/06)	1.00
Byung Suk Yang (7/1/07 - 5/31/08)	0.25
FTE Equivalent:	**5.05**
Total Number:	**12**

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Sugih Jamin	0.14	No
Jignesh Patel	0.14	No
Morley Mao	0.08	No
FTE Equivalent:	**0.36**	
Total Number:	**3**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
Brenden Blanco (8/18/05 - 3/25/06)	0.50
Joseph Flint (10/21/06 - 4/21/07)	0.50
Neil Pankey (4/22/06 - 4/21/07)	0.50
Jeffrey Parker (4/22/06 - 4/21/07)	0.50
Robert Sprentall (7/25/07 - 12/1/07)	0.50
FTE Equivalent:	**2.50**
Total Number:	**5**

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period:	5.00
The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:......	5.00
The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:......	0.00
Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):......	4.00
Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:......	0.00
The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense	0.00
The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:	0.00

Names of Personnel receiving masters degrees

NAME	
Mathew England	
John Umbaugh	
Todd Hopfinger	
Jeffrey Powers	
Patrick Turley	
Krian Upatkoon	
Byung Suk Yang	
Total Number:	**7**

Names of personnel receiving PHDs

NAME	
Hyunseok Chang	
Yun Chen	
Wenjie Wang	
Zhiheng Wang	
Total Number:	**4**

Names of other research staff

NAME	PERCENT_SUPPORTED	
Melinda Larocca (10/23/06 - 12/31/07)	0.10	No
Beverly Monaghan (9/19/05 - 9/30/06)	0.10	No
Lisa Wiltse (9/1/06 - 7/14/08)	0.10	No
FTE Equivalent:	**0.30**	
Total Number:	**3**	

Sub Contractors (DD882)

Inventions (DD882)

WebBee: A Platform for Secure Coordination and Communication in Crisis Scenarios

Wednesday, April 16, 2008

The Webbee Team, University of Michigan[1]

Abstract

Recently, disaster scenarios and terrorist attacks have made apparent some fundamental shortcomings in first responders' conventional coordination infrastructures. For example, unsatisfactory device connectivity, and security vulnerabilities made manifest by devices' inherently mobile nature, have the potential to seriously compromise first responders' effectiveness. To address these shortcomings, we designed and built *Webbee*, our secure coordination and communication infrastructure. In this article, we will take a high-level look at Webbee's architecture, and examine some interesting, non-trivial sample applications we have deployed on top of it.

Keywords: Webbee, disaster relief, instant infrastructure, GPS, database triggers, challenge response, quorum

1 Introduction

Ever since the September 11, 2001 terrorist attacks, the United States has been reevaluating coordination for first responders in disaster scenarios. First responders must communicate reliably and securely in times of crisis. However, communication channels like cell phone networks may not be appropriate during disaster scenarios: they may have been impaired or destroyed. Even if communication were *technically* feasible through these channels, extreme congestion might render them useless for first responders. Another problem is that these channels are more vulnerable to compromise: a malicious agent could steal a first responder's cell phone and intercept communications. This can seriously undermine first responders' effectiveness in crisis situations.

The problem is threefold. Firstly, responders must be able to communicate using devices they likely already have and are well-accustomed. Secondly, the communication channel must be secure in mobile environments. Finally, while in a time of crisis, the consumer communication infrastructure can sometimes be used, it cannot be relied upon solely. Webbee addresses each of these concerns.

2 Architecture

[1] **Primary Investigators:** Sugih Jamin, Zhuoqing Mao, T. V. Lakshman, Sarit Mukherjee, Jignesh Patel, Limin Wang. **Students, past and present:** Brendan Blanco, Hyunseok Chang, Yun Jason Chen, Søren Dreijer, Matt England, Joe Flint, Alex Garcia, Dan Harris, Todd Hopfinger, Dan Konson, Neil Panky, Jeff Powers, Bob Sprentall, Patrick Turley, John Umbaugh, Krian Upatkoon, Wenjie Wang, Zhiheng Wang, Byung Suk Yang

There are three major components of the Webbee architecture: the *instant infrastructure*, the *Webbee Coordination Server*, and the *database server* ***(Figure 1)***. The system has been designed so that components can be distributed across different machines.

Certain field personnel are equipped with battery-operated *Instant Infrastructure* backpack units. Equipment is commercial off-the-shelf hardware, so very large numbers of personnel can be outfitted easily. Custom SMesh software **[1]** helps maximize connectivity by dynamically reorganizing the network topology as personnel move about the field. The *Webbee Coordination Server* is an abstraction of several components that coordinate request handling, challenge-response management, policy examination, application hosting, and message dispatching. The *Database Server* manages all data interactions.

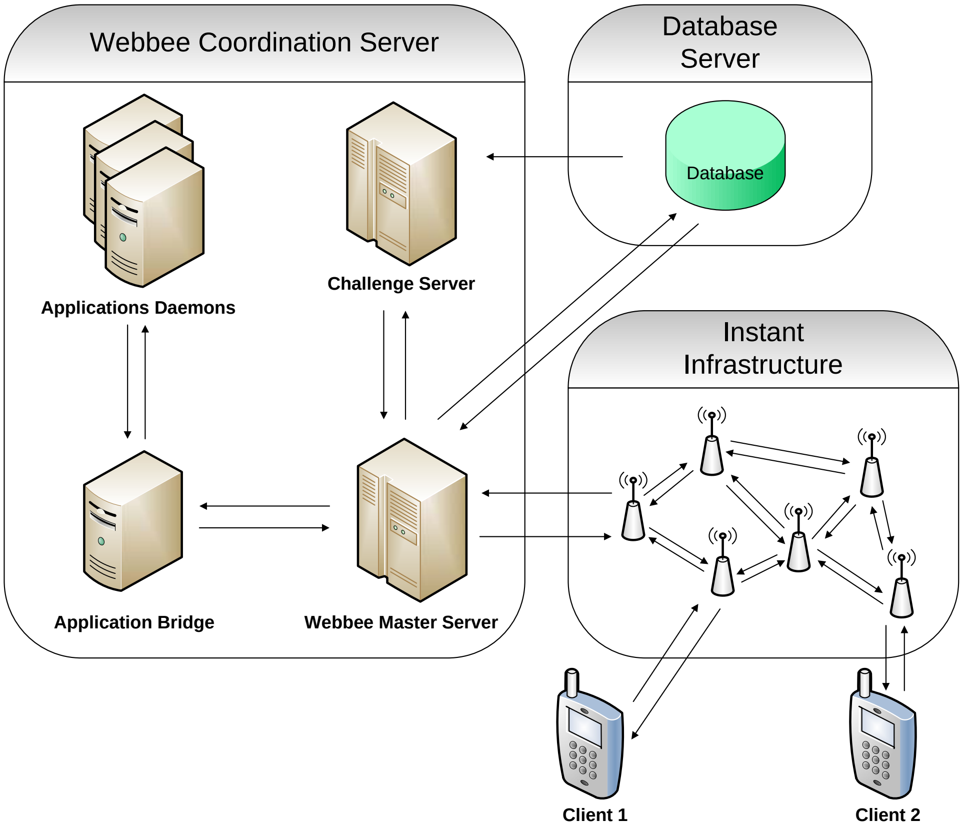


Figure 1: Webbee Component Architecture

3 Webbee Coordination Server Component Detail

3.1 Webbee Master Server and Challenge Server Interaction

The Webbee Master Server negotiates traffic from clients between the Challenge Server and the Application Bridge. When a client request comes in, the Webbee Master Server stores it, and asks the Challenge Server whether the client needs to be challenged. If the Challenge Server determines no challenge is needed, it tells the Webbee Master server that it is OK to proceed. Otherwise, the Challenge Server issues a challenge through the Master Server to the client. The client's solution is sent back through the Master Server to the Challenge Server. If it is invalid, the Challenge Server informs the Master Server that no action is to be taken, and the client is informed that that request was denied. If the solution is valid, the Webbee Master Server retrieves the client's most recent request and dispatches it to the Application Bridge. Our model, therefore, assumes that clients will only ever need a single request serviced at a time.

3.2 Security

Our security mechanism is broken into three separate subsystems: the Challenge Server, upload security, and download security. All are wrapped in a Secure Sockets Later (SSL).

3.2.1 The Challenge Server

The Challenge Server's job consists of *policies* and *challenges*. Policies encode conditions under which challenges are required, and are arranged in a hierarchy: if an agent passes one policy, there may still be subsequent policies that must be evaluated. The policy scheme for the Webbee Coordination Server is depicted in the flowchart in ***Figure 2.***

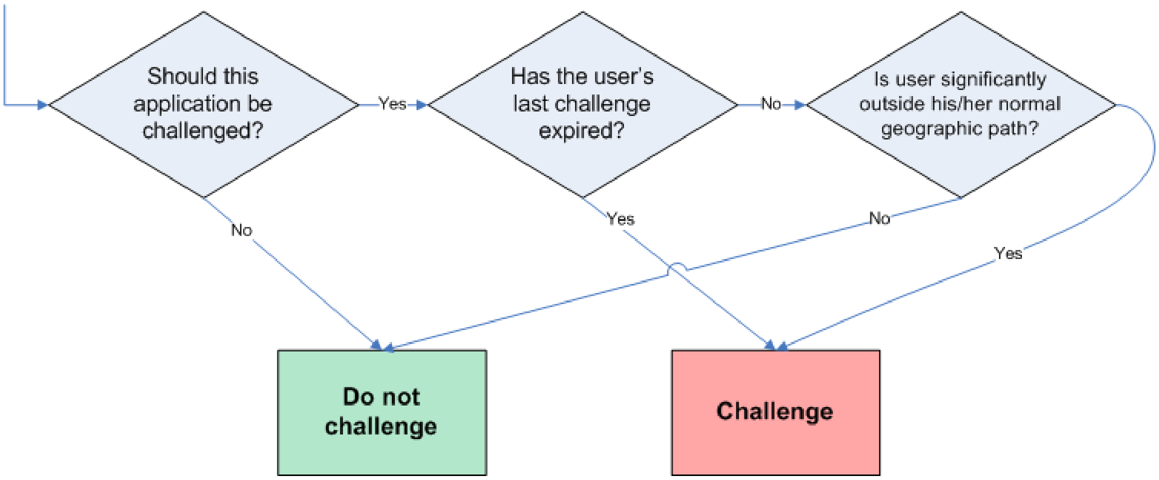

Should this application be challenged?
Yes
Has the user's last challenge expired?
No
Is user significantly outside his/her normal geographic path?
No
Yes
No
Yes
Do not challenge
Challenge

Figure 2: Policy Flowchart for The Webbee Coordination Server

The first policy here is an *application-level* test. This special policy grants full access to certain applications, and demonstrates that Webbee supports both secure and non-secure applications. If the application must be challenged, a *temporal* policy is activated to determine if the client's last challenge-response has expired. If it *has* expired, the client is issued a challenge. The last policy is a *geospatial* policy: if the user has strayed far away from the set of last known Global Positioning System (GPS) coordinates, the client is challenged.

Policy intervals can be defined on a per user basis, based on the level of security required for each client. At most, one challenge will occur through a traversal of this policy flowchart. Once the client solves the challenge, his or her GPS coordinates and a timestamp are stored in the database.

When the policy flowchart determines that a challenge is required, the server randomly selects one of several possible challenges and issues it to the client. If the client solves it, then the request is serviced. Otherwise, the current and all subsequent requests will also be denied until the client successfully solves the original challenge. This eliminates malicious clients' ability to game the system by exploring the challenge space.

Currently, only text-based (e.g., password) challenges have been implemented. With the right hardware, the challenge system could be extended to issue other kinds of challenges, such as biometric challenges, including fingerprint, voice, and/or retinal scanning.

3.2.2 Upload Security

In our scalable crisis management system, we are assuming that there are many downloads, but relatively few uploads. With this in mind, we have decomposed our security requirements into upload and download security characteristics.

For upload security, if a handheld is lost, we want to ensure that 1) data that has already been posted cannot be repudiated, and 2) data cannot be post-dated. Our forward secure signatures use a private key that evolves as a function of time; the public key, however, remains the same. This kind of forward secure scheme was proposed by Anderson **[2]** and implemented by Bellare and Miner **[3]**.

3.2.3 Download Security: The Quorum System

For download security, scaling is an important issue. If a client, we want to require relatively few clients to have to acquire new keys. The *Quorum* system implements download security with these kinds of scalability concerns in mind.

In *Quorum*, agents need to have a minimum number, k, of *keyshares* to securely read a message. At initialization, each agent receives m keyshares, where $m > k$, from a global keyshare set consisting of a total of s keyshares. If a user leaves, his or her shares are invalidated for *all* users. When a user has fewer than k valid shares, s/he must obtain a new set of valid keyshares from the global keyshare collection.

When the server broadcasts a message, it first encrypts it under a *message key*. This key, in turn, is itself encrypted s times. The s encrypted message keys and the encrypted message are all sent to all agents, who decrypt the message keys using their personal keysets. If exactly k of the keys are identical, it is valid and the agent proceeds to decrypt the encrypted message with that decrypted message key.

Figures 3.1 through ***3.3*** depict a scenario in which $k = 3$ and $m = 5$. In ***Figure 3.1***, Amanda, Bob, and Carl all have a quorum of valid keyshares. In ***Figure 3.2***, when Bob leaves, three of Amanda's keyshares are invalidated, forcing her to obtain new shares. Carl only has two shares invalidated; he can continue to operate. ***Figure 3.3*** depicts the scenario in which Amanda has reported a lost or stolen handheld, in which case all of Amanda's keyshares are invalidated. In this instance, Carl must reacquire new keyshares to operate.

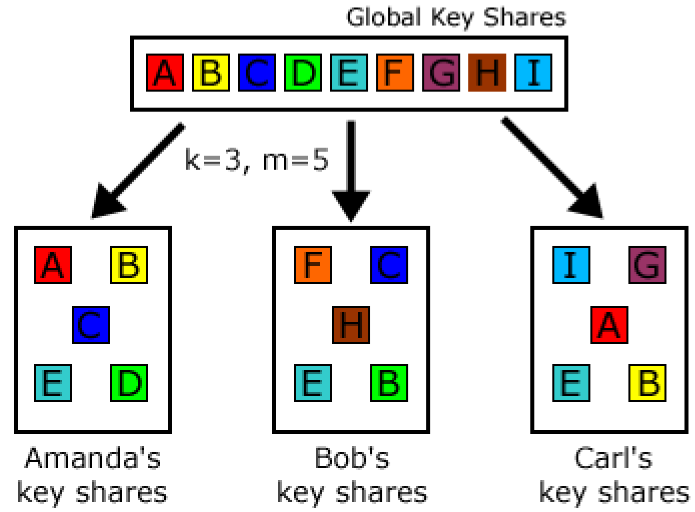


Figure 3.1: Amanda, Bob, and Carl initially all have valid keyshares

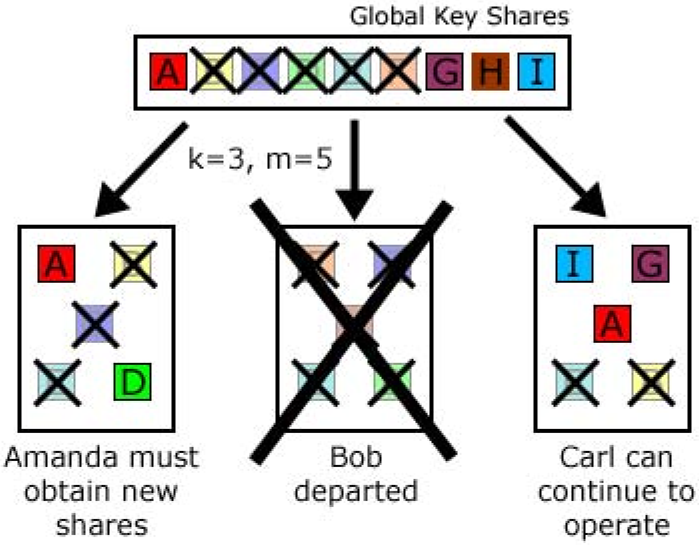


Figure 3.2: Bob leaves

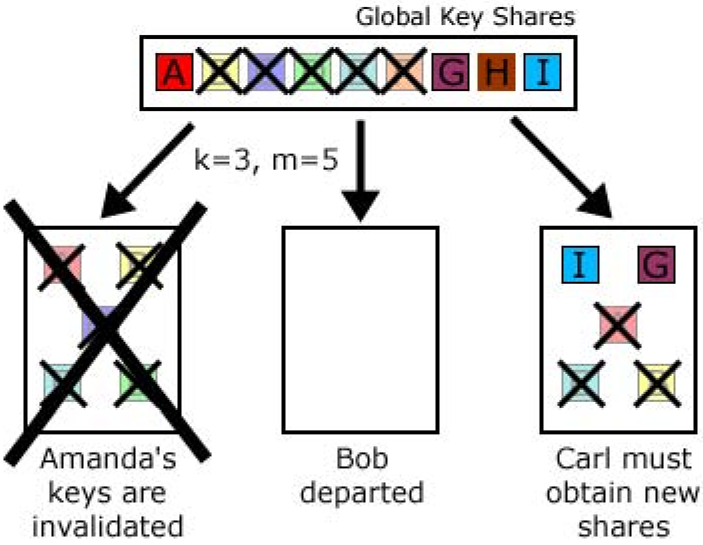


Figure 3.3: Amanda reports lost or stolen handheld

3.3 Application Bridge

The Application Bridge dispatches requests to the appropriate Application Daemon via an ID embedded in the request header. If a response is generated, it is sent back through the Webbee Master server to the client. *Gas Prices*, *Event Reports*, and *AC^2* are three applications we have built using the Webbee framework.

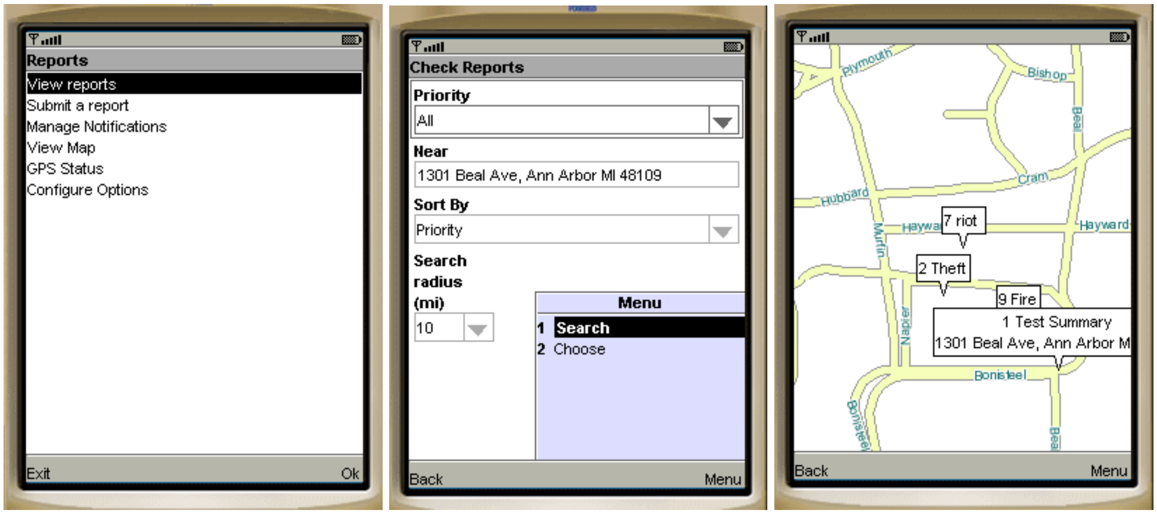
3.4 Gas Prices

The *Gas Prices* application allows clients to determine the gas stations with the cheapest prices. A client initially sends a request containing his or her GPS coordinates. The *Gas Prices* daemon constructs a map through an implementation of the U.S. Census Bureau's Topologically Integrated Geographic Encoding and Referencing system (TIGER) GIS database **[4]**, then queries a website that publishes up-to-date gas prices, and sends it back to the client.

Gas Prices and other applications use the Webbee scraping engine to obtain data from the web. For each application, a *scraping script* identifies the data components of interest in a webpage. Any static or dynamic data can be acquired – including text, images, and audio.

3.5 Event Reports

The *Event Reports* application in (***Figure 4)*** allows clients to log incidents that they observe in the field. Other clients are notified about these incidents only once they become geospatially relevant. Clients specify details about an incident by typing out a short message – as well as a radius in meters - on the handheld device. As other clients move in range, their handhelds are notified via the Short Messaging Service (SMS). This relieves clients of having to sift through reports to determine which are immediately important, enabling him or her to react faster and more effectively.



Reports

View reports
Submit a report
Manage Notifications
View Map
GPS Status
Configure Options

Exit Ok

Check Reports

Priority: All

Near: 1301 Beal Ave, Ann Arbor MI 48109

Sort By: Priority

Search radius (mi): 10

Menu
1 Search
2 Choose

Back Menu

Figures 4.1, 4.2, and 4.3: Mobile client screenshots for the Event Reports system

A scenario is shown in ***Figure 5***. A report about a fire is submitted at the Chicago Mercantile Exchange *(A)*. One Fire Department unit *(B)* and two Police Department units *(C)* and *(F)* receive the alert about the fire. Another report about an unrelated incident is submitted by an informant across the city *(D)*. Here, one Fire Department unit is alerted *(E)*, as is one Police Department unit *(F)*. Notice that *(F)* receives alerts about both incidents, since it is in range of both. In contrast, *G* receives no alerts. As soon as *G* moves into range (if ever), s/he will receive the report.

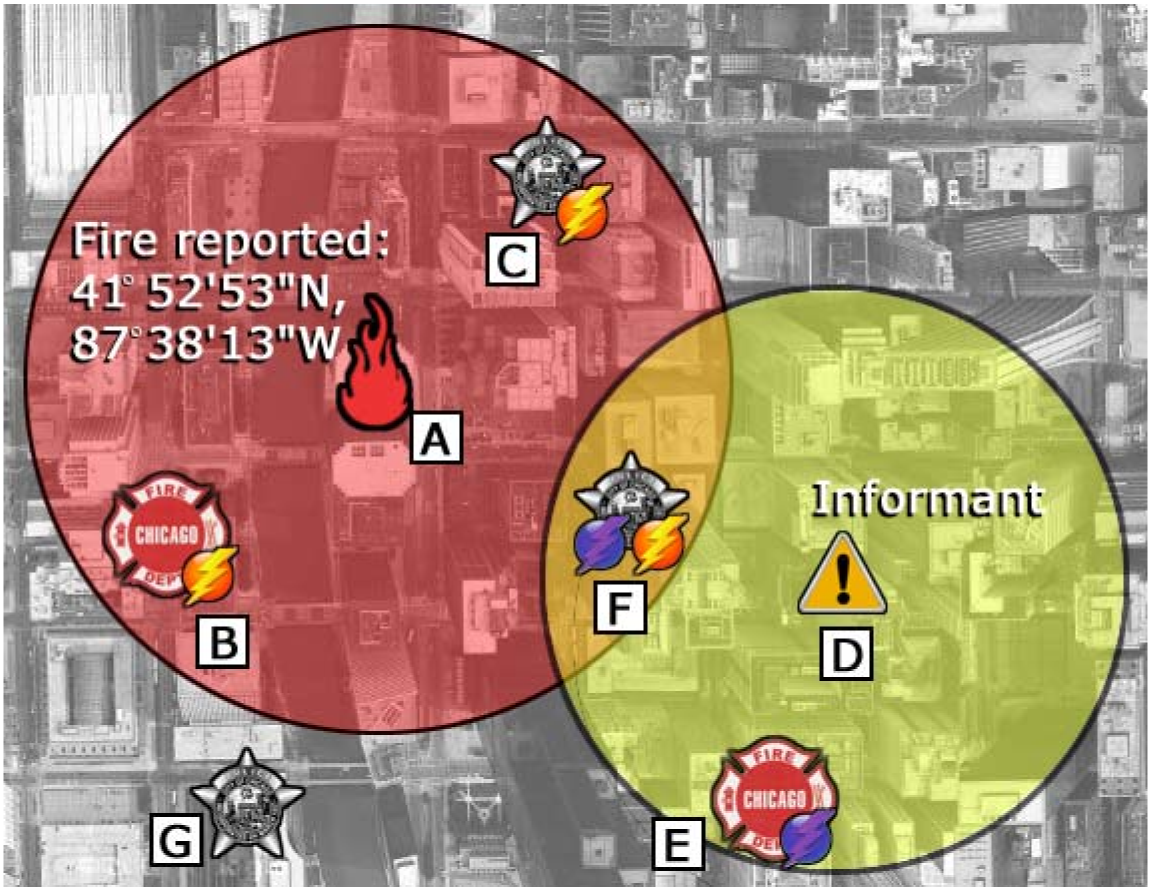


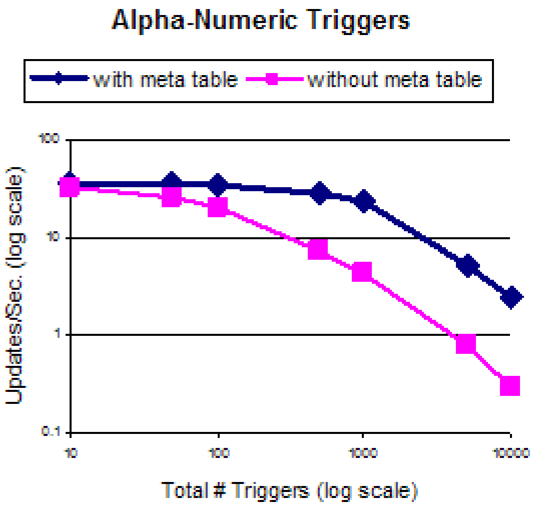
Figure 5: an example Event Reports scenario

3.5.1 Event Reports - exploiting database triggers for better performance

Report notifications to clients are implemented through database triggers. The Webbee Database Server contains an Information Server, which is a Postgres database with PostGIS **[5]** extension, that is integrated with an instance of a Visualization Server in an application daemon. The Visualization Server renders map data for visualization **[6]** in concert with an instance of a TIGER database **[4].** When a client enters an event report region, the database triggers the insertion of a new record into a special table. Meanwhile, the event reports daemon monitors this table. If there are any new entries, the daemon creates an SMS and sends it to the target user. The heavy lifting for this mechanism is done through an extension of Postgres triggers ***(Figures 6.1 and 6.2)***, resulting in fewer queries and better performance.

Trigger support in Postgres is table-based and comparatively primitive: with *n* table triggers, an update will cause *n* operations to occur, resulting in decreased performance if updates are frequent. Also, Postgres does not provide out-of-the-box support for multi-table triggers. This becomes a problem, for example, with mixed notifications.

To address these problems, we have implemented a *trigger meta table*, which encodes relationships between trigger class identifiers and ownership, and is referenced before trigger evaluations. Consider the mixed notification: “NOTIFY me WHEN I come WITHIN 2 miles of a gas station WITH gas price LOWER THAN $2.50.” When the user’s location is updated, the trigger meta table is examined on the user id trigger class identifier. When gas prices are updated, entries in the meta table are examined on the gas station id and the trigger class identifier. Performance is up to 8X faster than without the meta table for alpha-numeric triggers, and up to 10X faster for spatial range triggers. Performance increases as the total number of triggers increases ***(Figures 6.1, 6.2*****)**.



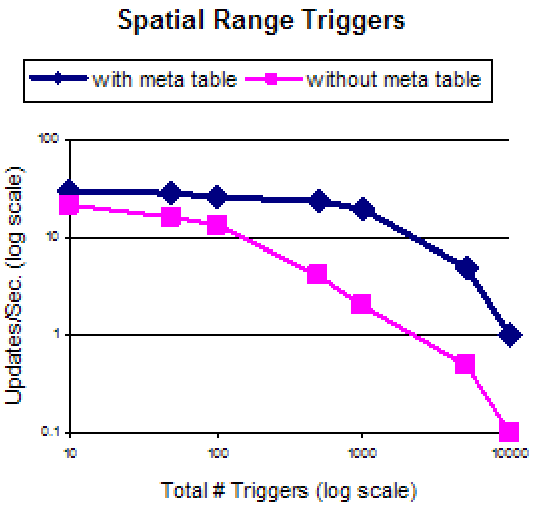


Figure 6.1: Meta table performance comparison for alpha-numeric triggers

Figure 6.2: Meta table performance comparison for spatial range triggers

3.6 Agent Contingency and Action Coordinator (AC^2)

Another application that we have built is an *Agent Contingency and Action Coordinator (AC^2)* application, which provides a full text, voice, and picture messaging system. Messages may be sent directly to individual clients or by *radius*. The radius message mechanism works as follows: the sender specifies his or her GPS coordinates and radius in meters within the message header. When the message is sent to the server, all agents’ last known GPS coordinates are examined. The message is sent to all agents in the defined circle. Radius messaging might be useful, for example, for the dissemination of orders to all agents within a specific location.

Another innovative feature of AC^2 is *message withdrawal*. If a client has sent a message, and then later circumstances change and s/he no longer wants the message consumed by other agents, s/he can withdraw the message: the message will be removed from the inboxes of all agents to whom the user sent it. This is useful in situations in which agents have decided a reported incident has stopped being of interest. For example, if an agent initially reports seeing a suspicious package, but later determines that it is not a threat, s/he can withdraw the message to prevent confusion among the other agents. All messages – including withdrawn messages – persist in the Webbee server log so as to provide a traceable audit trail.

4 Conclusion

Webbee is a robust, mobile, scalable communications and coordination framework that can handle several applications at various levels of security. The Challenge-response and Quorum systems are scalable mobile security paradigms that are appropriate for our system. The implementation of a policy hierarchy strikes a nice balance between client situation-dependent security and future extensibility. Finally, database optimizations like trigger meta tables and streamlined indexing impart significant performance gains to our system.

5 References

[1] Distributed System and Networks Lab. *SMesh*. Johns Hopkins University. 2008. <http://www.smesh.org>

[2] Anderson, R. Invited Lecture. *Fourth Annual Conference on Computer and Communications Security*, 1997.

[3] Mihir Bellare and Sara K. Miner. "A forward-secure digital signature scheme." *Lecture Notes in Computer Science*, 1666:431-448, 1999.

[4] *Topologically Integrated Geographic Encoding and Referencing system*. United States Census Bureau. 2008. <http://www.census.gov/geo/www/tiger/index.html>

[5] *PostGIS*. Refractions Research. 2007. <http://postgis.refractions.net/>

[6] *MapServer*. University of Minnesota. 2008.
<http://mapserver.gis.umn.edu/>